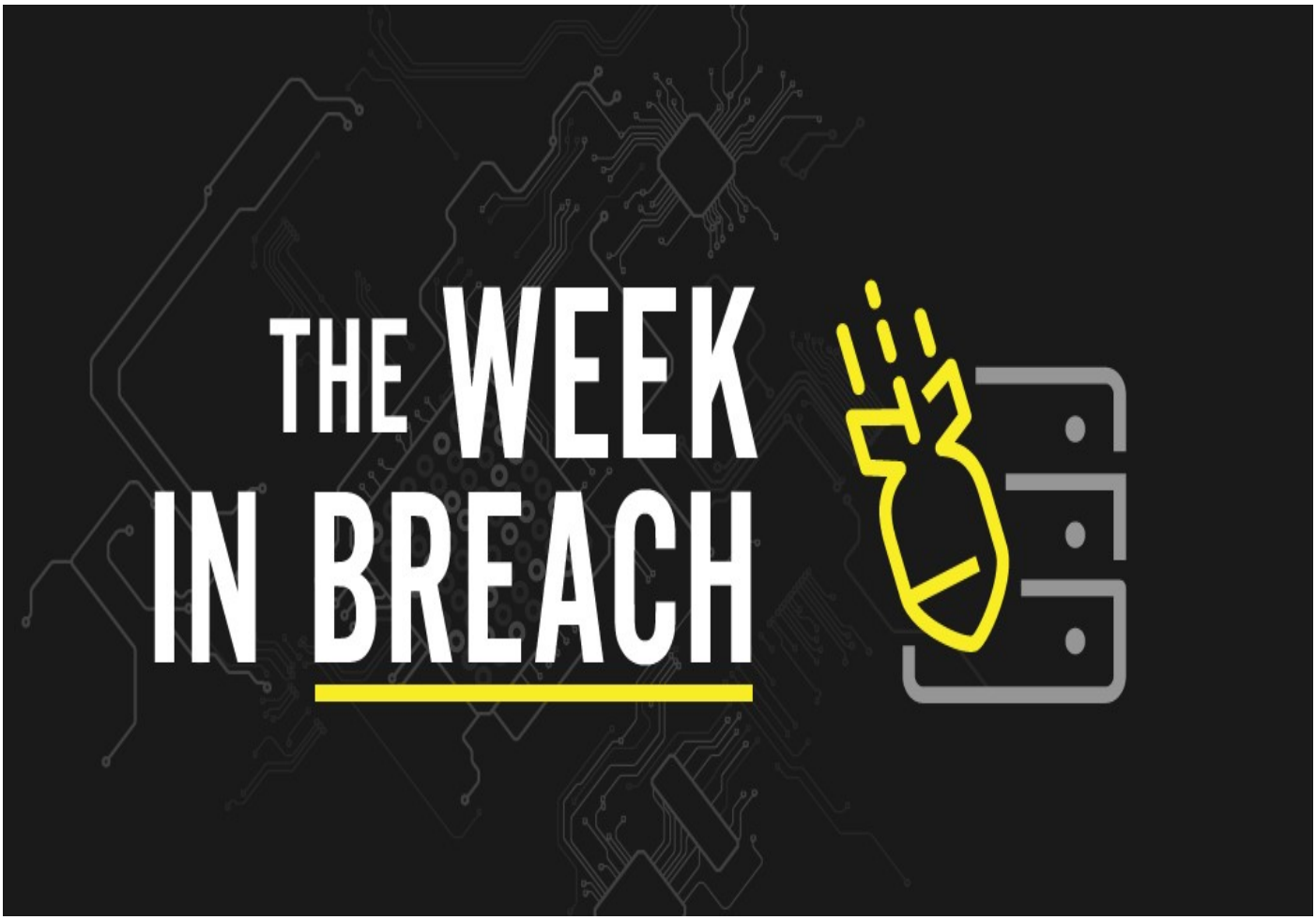
THE WEEK IN BREACH NEWS: 05/03/23-05/09/23

DenBe Computer Consulting
Connecting Business

May 10th 2023 by Dennis Jock



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

Americold
https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-outage-caused-by-network-breach/

Exploit: Ransomware

Americold: Cold Storage Company

Risk to Business: 1.422 = Extreme

Americold, a leading cold storage logistics company, announced that it has experienced a network outage as the result of a cyberattack. The incident began last Tuesday night and has persisted, leaving employees and customers scrambling. The company has asked customers to cancel inbound deliveries and to reschedule all but the most critical outbound deliveries. Americold expects to have systems restored late this week. Americold said that it is focused on rebuilding affected systems, leading to speculation that this is a ransomware incident. They expect to restore most services this week.

How It Could Affect Your Business: Logistics companies are a key element in the supply chain, making them highly attractive targets for bad actors.

United HealthCare
https://www.cbsnews.com/losangeles/news/united-healthcare-reports-data-breach-that-may-have-revealed-customers-personal-information/

Exploit: Hacking

United HealthCare: Insurer

Risk to Business: 1.762 = Severe

Health insurance giant United HealthCare has informed members that it has experienced a data breach. The problem was uncovered on February 22, 2023, when United identified suspicious activity on its local app that may have led to the disclosure of members' personal information. The company estimates that the breach happened between February 19 and February 25, 2023. Members may have had personal information exposed in the breach including first and last names, health insurance member ID numbers, dates of birth, addresses, dates of service, provider names, claim information and group names and numbers. UnitedHealthcare said that Social Security and driver's license numbers were not exposed. Affected members have been informed via letter.

How It Could Affect Your Business: This kind of incident will end up costing United HealthCare a fortune after regulators in multiple states and at the federal level get through with them.

Fincantieri Marine Group (FMG)
https://www.infosecurity-magazine.com/news/us-navy-contractor-cyberattack/

Exploit: Ransomware

Fincantieri Marine Group (FMG): Shipbuilder

Risk to Business: 1.681 = Severe
U.S. Navy contractor Fincantieri Marine Group (FMG) experienced a ransomware attack last week that is causing a temporary disruption to certain computer systems on its network. A company spokesperson said that the ransomware attack on the Fincantieri Marinette Marine shipyard disrupted operations across the shipyard by rendering data on network servers unusable as well as impacting critical CNC (Computer Numerical Control) manufacturing machines. The company said that it doesn't have any indication that employee data was compromised. The incident is under investigation.

How It Could Affect Your Customers' Business: Strategic attacks that impair defense manufacturing are a dangerous modern hazard that companies must be ready for.

The Diocese of Las Vegas
https://www.ktnv.com/news/some-sensitive-information-potentially-compromised-diocese-of-las-vegas-reports-cybersecurity-breach

Exploit: Hacking

The Diocese of Las Vegas: Religious Organization

Risk to Business: 1.919 = Severe

Late last week The Diocese of Las Vegas admitted that it had experienced a data breach that may have exposed sensitive data. The breach was discovered on March 12, 2023, and concerned data held by the Diocese about its volunteers, parishioners, donors and others. The Diocese did not specify exactly what types of information were stolen, but it was quick to reassure the public that employee payroll and benefits information and Catholic Stewardship Appeal information were not impacted. The incident has been reported to the relevant authorities.

How It Could Affect Your Customers' Business: Churches and non-profits must be just as vigilant against cyberattacks as businesses because they're just as much in the line of fire.

CIC Group, Inc.
https://thecyberwire.com/newsletters/privacy-briefing/5/80

Exploit: Hacking

CIC Group, Inc.: Engineering and Construction Manufacturing

Risk to Business: 1.781 = Severe

CIC Group, Inc. a commercial and industrial business holding company based in St. Louis, Missouri, has disclosed that it was recently the victim of a cyberattack. In a filing with the Texas Attorney General's Office, CIC Group said that an unauthorized party had gained access to confidential customer information that the company was holding including consumers' names, addresses and Social Security numbers. The company has begun sending out data breach notification letters to everyone who was impacted by the incident.

How It Could Affect Your Customers' Business: Supply chain attacks have been escalating, bringing fresh danger to businesses in every sector.

The Minneapolis Public Schools
https://gizmodo.com/ransomware-gang-medusa-data-breach-minneapolis-school-a-1850380421

Exploit: Ransomware

The Minneapolis Public Schools: Education Authority

Risk to Business: 1.336 = Extreme

A mid-March ransomware attack has resulted in highly sensitive data about and belonging to thousands of public school students in Minneapolis being exposed on the dark web. The ransomware group Medusa claimed responsibility for the attack and began releasing information on its dark web leak site last week. Many students' identifying data including birthdays and Social Security numbers was exposed, but that's not the most sensitive data by far. The torrent of an estimated 200,000 files stolen from includes data about incidents of students exhibiting behavioral issues, documentation of problems at home like divorcing or incarcerated parents, data about conditions like Attention Deficit Disorder, documented indications of injuries, results of intelligence tests and what medications they take. Documents detailing allegations of abuse by district staff are also in this tranche, including the accusing student's name, date of birth and address.

How It Could Affect Your Customers' Business: This is a horrible story that illustrates the human cost and cruelty of many cyberattacks.